

Appl. No. 09/785,722
Amdt. Dated June 14, 2005
Reply to Office Action of April 14, 2005

Docket No. CM04812H
Customer No. 22917

REMARKS/ARGUMENTS

Applicants have amended Claims 1, 2, 6, 8, 13, 16, 20, 23, 24, 27, 29, 33, 36, 40, 42 and 68 and have cancelled Claims 7, 9, 28, 30, 51 and 72. Claims 1-6, 8, 10-27, 29, 31-50, 52-71, 73-91, 93 and 94 remain in this application. No new matter was added by these amendments. Reconsideration of this application is respectfully requested in view of the above amendments and these remarks/arguments.

The Examiner has rejected Claims 1-6, 8, 10-12, 14-19, 21-27, 29, 31, 32, 34-39 and 41 under 35 U.S.C. 102(e) as being anticipated by "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000. The Examiner has further rejected Claims 7, 9, 13, 20, 28, 30, 33, and 40 under 35 U.S.C. 103(a) as being unpatentable over the TETRA-2000 reference. Applicants have cancelled Claims 7, 9, 28 and 30, thereby rendering moot the Examiner's rejection of these claims. Applicants traverse the remaining rejections. Applicants submit that the TETRA-2000 reference does not anticipate Claims 1-6, 8, 10-12, 14-19, 21-27, 29, 31, 32, 34-39 and 41 and does not render Claims 13, 20, 33 and 40 obvious because it fails to teach or suggest all of the elements recited in or included by dependency in these claims.

More specifically, applicants have amended Claims 1 and 23 to include the limitations from cancelled dependent Claims 7, 9, 28 and 30 of "encrypting the derived cipher key using an intrakey." Applicants have further amended Claims 16 and 36 to include the limitations deleted from dependent Claims 20 and 40, respectively, of "receiving a derived cipher key, which is encrypted by an intrakey." The Examiner argues in paragraphs 55-64 of the current Office Action that the TETRA-2000 reference, at Section 6.5.1.3 and Section 4.2.3 lines 8-9, teaches these above-referenced limitations recited in Claims 1, 16, 23 and 36, and in particular that the TETRA-2000 reference can be used as either an interkey or an intrakey depending on the CCK-id and that it would have been obvious to a person of ordinary skill in the art to use a CCK (an intrakey) to encrypt a derived cipher key which reads on the above-recited limitations of Claims 1, 16, 23 and 36. Applicants disagree.

The TETRA 2000 reference specifically defines a CCK in section 3.1 as a "cipher key that is generated by the infrastructure to protect group addressed signaling and traffic. . . [and] to protect[] SSI identities (EST) in layer 2." This reference further defines a derived cipher key as

Appl. No. 09/785,722
Amtd. Dated June 14, 2005
Reply to Office Action of April 14, 2005

Docket No. CM04812H
Customer No. 22917

"for use in protection of individually addressed signaling and traffic." Thus, based on these definitions, the TETRA-2000 reference does not teach or suggest using the CCK to protect a derived cipher key since a derived cipher key is not "group addressed signaling and traffic" or "ESI," which are the only two items defined in the reference as being protected by a CCK. Moreover, the CCK-Id is defined in the TETRA-2000 reference at section 3.1 as "the identification of the [CCK] key with an LA [location area] and the protection against replays of old keys." Thus the CCK-Id does not function to identify the CCK as either an intrakey or an interkey as the Examiner suggests, it merely serves to associate the CCK to a particular LA and to protect against outdated CCKs being used in the system.

For all of these reasons, Applicants submit that Claims 1, 16, 23 and 36 are now in a condition for allowance and that Claims 2-6, 8, 10-15, 17-22, 24-27, 29, 31-35 and 37-41, which depend from Claims 1, 16, 23 and 36, are allowable for all of the same reasons above associated with these independent claims.

The Examiner has rejected Claims 42, 68-69, 71-82, 87-91 and 93-94 under 35 U.S.C. 102(c) as being anticipated by Matsumoto (USPN 6,134,431), hereinafter referred to as Matsumoto. Applicants have cancelled Claim 72, thereby rendering moot the Examiner's rejection of this claim. Applicants traverse the remaining rejections. Applicants submit that Matsumoto does not anticipate Claims 42, 68-69, 71, 73-82, 87-91 and 93-94 because it fails to teach or suggest all of the elements recited in or included by dependency in these claims.

More specifically, amended Claim 42 includes the limitation of "a second key, which is an interkey, for encrypting at least a segment of the first zone session authentication information for transport to a system device in a zone other than the first zone." That the second key is an interkey is a limitation that was added into Claim 42 from cancelled Claim 51. Thus, the Examiner did not contend that Matsumoto taught this limitation but contended that the TETRA-2000 reference taught this limitation from Claim 51 (see paragraph 79 of the pending Office Action). Essentially, the Examiner argues that the CCK can be used as an intrakey or an interkey depending on the CCK-Id. Applicants disagree.

Applicants' specification defines an interkey as being "used to encrypt key material sent between pools or zones . . . or within a certain group of system devices." The MPEP provides that when the specification provides definitions for terms appearing in the claims that the specification can be used in interpreting claim language during examination. MPEP §2111.01.

Appl. No. 09/785,722
Amtd. Dated June 14, 2005
Reply to Office Action of April 14, 2005

Docket No. CM04812H
Customer No. 22917

Thus, by interpreting the term interkey in accordance with its definition as provided in the specification, Applicants submit that the TETRA-2000 reference does not teach the above-quoted language recited in Claim 42. More particularly, this reference does not teach that a CCK can be an interkey or an intrakey based upon its CCK-Id. As argued above, the TETRA-2000 reference gives a very specific definition for the term CCK and its use does not include those of the interkey as defined in the instant specification, namely, to encrypt key material sent between pools or zones . . . or within a certain group of system devices. Moreover, as argued above the TETRA-2000 reference also gives a very specific definition for the term CCK-Id, and its use does not include identifying a CCK as an interkey or an intrakey but, instead, is used simply to associate a CCK with a given location area and to protect against outdated CCKs being used in the system.

For all of the above reasons, Applicants submit that Claim 42 is now in a condition for allowance.

With respect to Claim 68, Applicants have amended this claim to include the limitation from cancelled dependent Claim 72 of "encrypting the session authentication information using an interkey." The Examiner argues that Matsumoto teaches this limitation at col. 24, lines 47-65. As stated above, an interkey is defined in the specification and should, thereby, be construed by the Examiner as being "used to encrypt key material sent between pools or zones . . . or within a certain group of system devices." There is no key defined in Matsumoto for performing this function. Moreover, the claim language in col. 24, lines 47-65 of Matsumoto does not describe an interkey for authenticating session authentication information. It simply describes a personal station storing a peculiar key for a first radio communication system when it enters a first closed service area and that the personal station stores a peculiar key for a second radio communication system when it enters a second closed service area. This language alone does not teach the above-quoted limitations recited in Claim 68.

For all of the above reasons, Applicants submit that Claim 68 is now in a condition for allowance and that Claims 69, 71 and 73-82 that depend from and include all of the limitations of Claim 68 are allowable for all of the same reasons associated with Claim 68.

Claim 87 also includes the limitation of "encrypt the session authentication information using an interkey" that the Examiner argues is taught in Matsumoto. Applicants disagree for all of the reasons stated above with respect to Claim 68. Therefore, Applicants submit that Claim

Appl. No. 09/785,722
Amtd. Dated June 14, 2005
Reply to Office Action of April 14, 2005

Docket No. CM04812H
Customer No. 22917

87 and Claims 88-91 and 93-94 that depend from and include all of the limitations of Claim 87 are allowable for all of the reasons above associated with Claim 68.

The Examiner has rejected Claims 42-65 and 67 under 35 U.S.C. 103(a) as being unpatentable over the TETRA-2000 reference in view of Matsumoto. Applicants have cancelled Claim 51, thereby rendering moot the Examiner's rejection of this claim. Applicants traverse the remaining rejections. Applicants submit that the combined teachings of the TETRA-2000 reference and Matsumoto do not render Claims 42-50, 52-65 and 67 obvious because the combined teachings fail to teach or suggest all of the elements recited in or included by dependency in these claims.

As argued above, amended Claim 42 includes the limitations of "a second key, which is an interkey, for encrypting at least a segment of the first zone session authentication information for transport to a system device in a zone other than the first zone," and this limitation is not taught in either the TETRA-2000 reference or in Matsumoto. Therefore, Claim 42 is now in a condition for allowance as well as Claims 43-50, 52-65 and 67, which depend from and include all of the limitations of Claim 42.

The Examiner has rejected Claim 70 under 35 U.S.C. 103(a) as being unpatentable over Matsumoto in view of Matyas (USPN 5,164,988), hereinafter referred to as Matyas. Applicants traverse this rejection. Applicants submit that the combined teachings of Matsumoto and Matyas do not render Claim 70 obvious because the combined teachings fail to teach or suggest all of the elements recited in or included by dependency in these claims. As argued above Claim 68, from which Claim 70 depends, recites the limitations of "encrypting the session authentication information using an interkey," which is not taught in Matsumoto nor in Matyas. Therefore Claim 70 is in a condition for allowance.

The Examiner has rejected Claim 66 under 35 U.S.C. 103(a) as being unpatentable over the TETRA-2000 reference in view of Matsumoto and in view of Matyas. Applicants traverse this rejection. Applicants submit that the combined teachings of the TETRA-2000 reference, Matsumoto and Matyas do not render Claim 66 because the combined teachings fail to teach or suggest all of the elements recited in or included by dependency in these claims. As argued above, Claim 42, from which Claim 66 depends, recites the limitations of "a second key, which is an interkey, for encrypting at least a segment of the first zone session authentication information for transport to a system device in a zone other than the first zone," which is not

Appl. No. 09/785,722
Amdt. Dated June 14, 2005
Reply to Office Action of April 14, 2005

Docket No. CM04812H
Customer No. 22917

taught in either the TETRA-2000 reference or in Matsumoto, nor in Matyas. Therefore Claim 66 is in a condition for allowance.

The Examiner has rejected Claims 83 and 84 under 35 U.S.C. 103(a) as being unpatentable over Chan (USPN 6,128,389), hereinafter referred to as Chan, in view of Jobst (USPN 6,707,915 B1), hereinafter referred to as Jobst. Applicants traverse these rejections. Applicants submit that the combined teachings of Chan and Jobst do not render Claims 83 and 84 obvious because the combined teachings fail to teach or suggest all of the elements recited in or included by dependency in these claims.

More specifically, Claim 83 recites the limitations of "wherein the home location register is arranged and constructed to continue to provide authentication and support secure communications in the event of a fault at any of the key management facility, user configuration server, and the zone manager." The Examiner contends the combination of a mobile phone identification (i.e., IMEI) and an MM IDENTITY REQUEST message taught in Jobst teaches these limitations. However, it is unclear how the examiner reaches this conclusion based solely on the language in col. 2, lines 28-33 of Jobst. Applicants submit that the IMEI is nothing more than a means to "uniquely identify the phone." With respect to the MM IDENTITY REQUEST message, Jobst states only that it may be given to "identify failures in the system (emphasis added)." Identifying a failure in a system is completely different from "continuing to provide authentication and support secure communications in the event of a fault" as recited in Claim 83.

For all of the above reasons, Applicants submit that Claim 83 and Claim 84, which depends from and includes all of the limitations of Claim 83, are in a condition for allowance.

The Examiner has rejected Claims 85 and 86 under 35 U.S.C. 103(a) as being unpatentable over Chan in view of Jobst and in view of the TETRA-2000 reference. Applicants traverse these rejections. Applicants submit that the combined teachings of Chan, Jobst and the TETRA-2000 reference do not render Claims 85 and 86 obvious because the combined teachings fail to teach or suggest all of the elements recited in or included by dependency in these claims. As argued above, Claim 83 from which Claims 85 and 86 depend recites the limitations of "wherein the home location register is arranged and constructed to continue to provide authentication and support secure communications in the event of a fault at any of the key management facility, user configuration server, and the zone manager," and neither Chan nor

Appl. No. 09/785,722
Amtd. Dated June 14, 2005
Reply to Office Action of April 14, 2005

Docket No. CM04812H
Customer No. 22917

Jobst teaches these limitations. The TETRA-2000 reference also does not teach these limitations. Therefore, Claims 85 and 86 are in a condition for allowance.

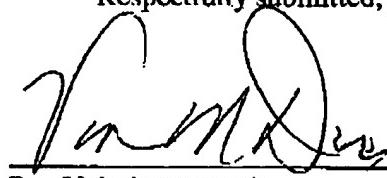
The Applicants believe that the subject application, as amended, is in condition for allowance. Such action is earnestly solicited by the Applicants.

In the event that the Examiner deems the present application non-allowable, it is requested that the Examiner telephone the Applicants' attorney or agent at the number indicated below so that the prosecution of the present case may be advanced by the clarification of any continuing rejection.

Accordingly, this application is believed to be in proper form for allowance and an early notice of allowance is respectfully requested.

Please charge any fees associated herewith, to Deposit Account No. 502117, Motorola, Inc.

Respectfully submitted,



By: Valerie M. Davis

Attorney of Record
Reg. No.: 50,203

Telephone: 847.576.6733
Fax No.: 847.576.0721

SEND CORRESPONDENCE TO:

Motorola, Inc.
Law Department
1303 E. Algonquin Road
Law Department
Schaumburg, IL 60196
Customer Number: 22917